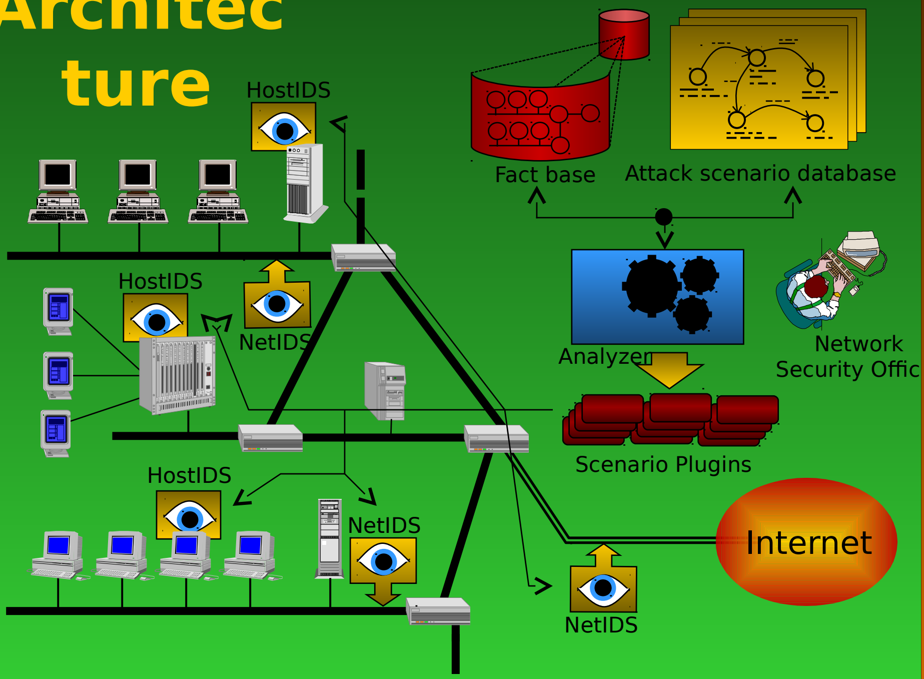
# NetSTAT

## A Model-based Real-time Intrusion Detection System for Large Scale Heterogeneous Networks

## Architecture



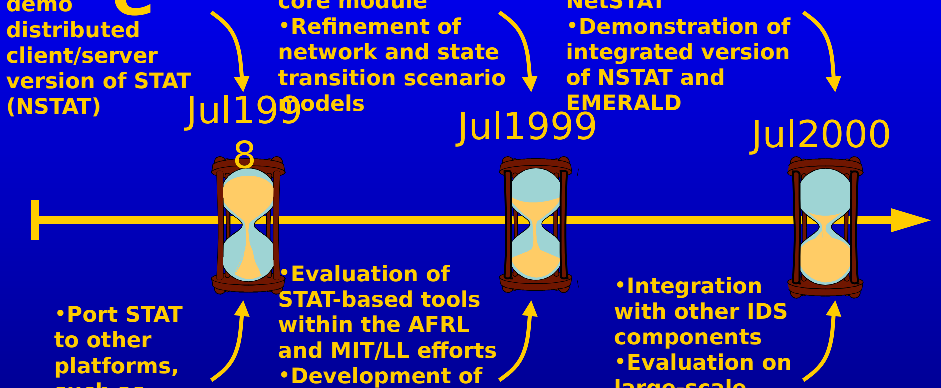
## New Ideas

- State/transition analysis of host-based *and* network-based attacks
- Core module that embeds domain-independent semantics of STAT
- Well-defined way to extend generic core to develop STAT-based IDSs
- Fact base with structured representation of protected networks and hosts
- Analyzer that customizes generic attack scenarios for target networks and hosts
- Automatic deployment and configuration of IDSs

## Impact

- Creation of a generic toolkit for the development of STAT-based IDSs
- Improved reusability, portability, and extendibility
- Optimization of critical functions delivers improved performance
- Support for the interoperability of IDSs in different domains and environments
- Focused and efficient real-time network intrusion detection in complex, large scale heterogeneous information system

## Schedule



**•Design and demo distributed client/server version of STAT (NSTAT)**

**•Complete STAT core module**
**•Refinement of network and state transition scenario models**

**•Enhancement of NetSTAT**
**•Demonstration of integrated version of NSTAT and EMERALD**

**•Port STAT to other platforms, such as DG/UX**

**•Evaluation of STAT-based tools within the AFRL and MIT/LL efforts**
**•Development of semantics for the attack specification language**

**•Integration with other IDS components**
**•Evaluation on large-scale heterogeneous information systems**

University of California, Santa Barbara: R.A. Kemmerer